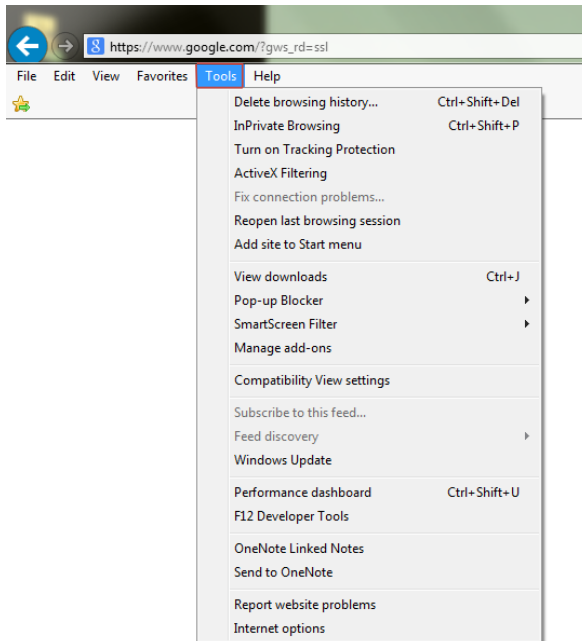


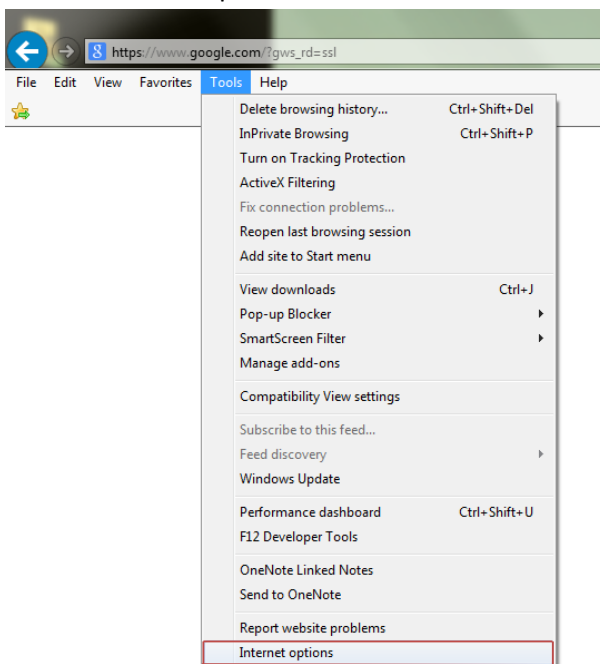
Configuring Internet Explorer for JTDI Access

This documentation will work for Internet Explorer 11 or lower.

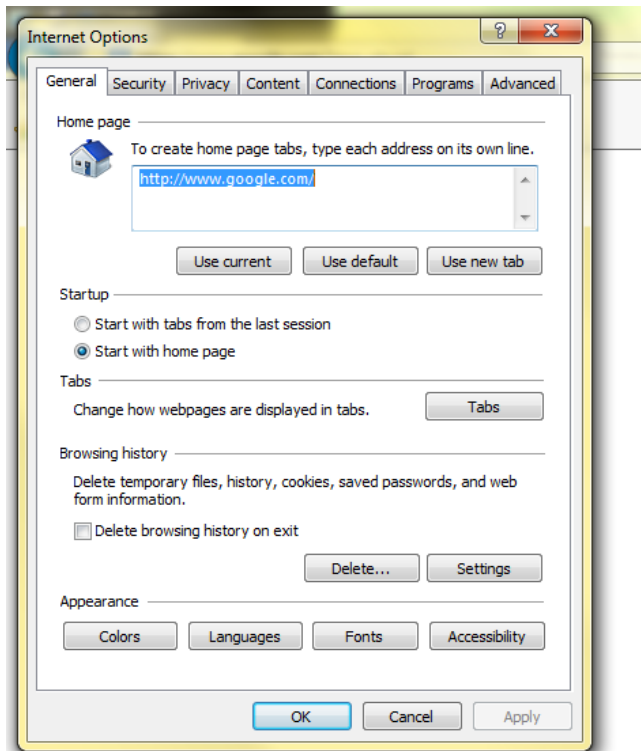
1. Open your web browser and select “Tools”



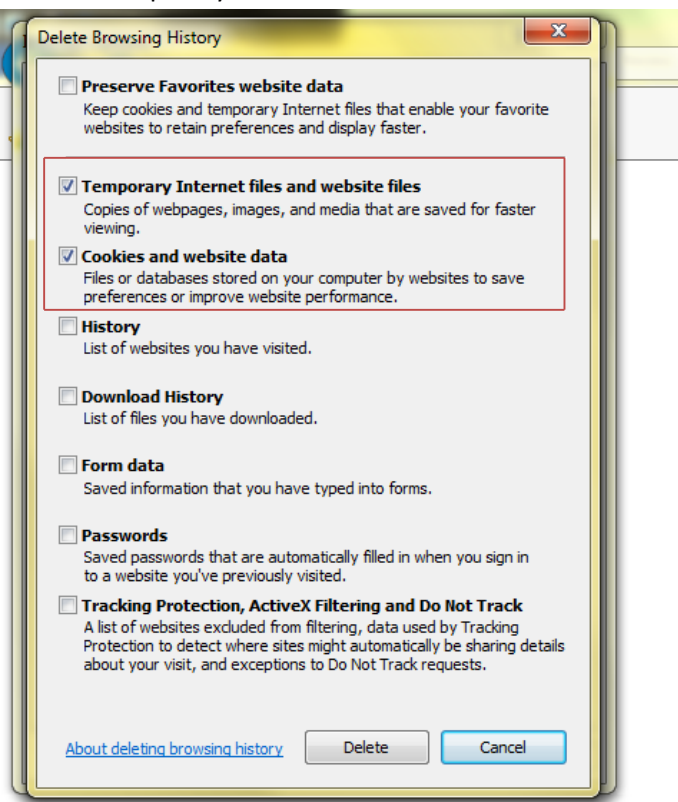
2. Select “Internet Options”



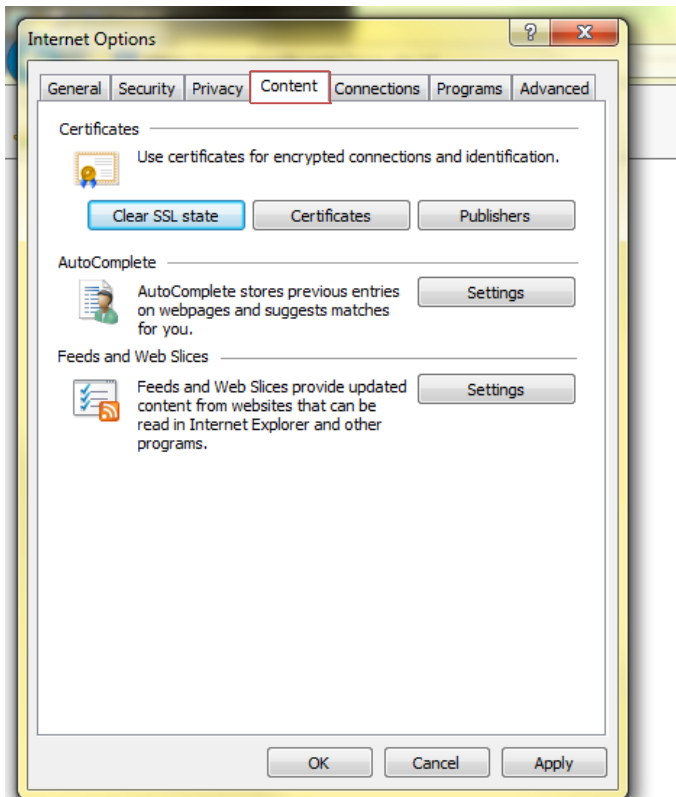
3. Select the “Delete” button in the browsing history section



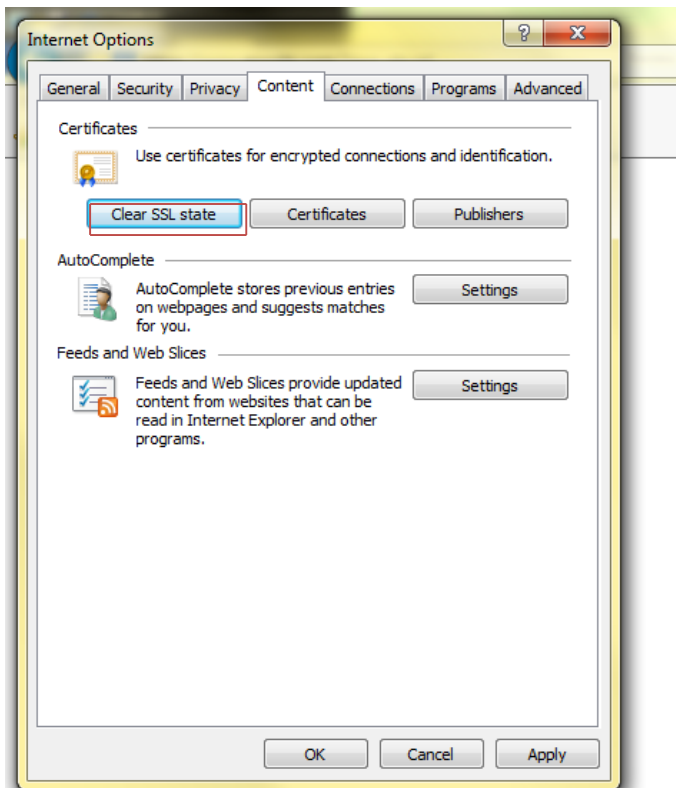
4. Delete “Temporary Internet files and website files” and “Cookies and website data”



5. Next select the “Content” tab



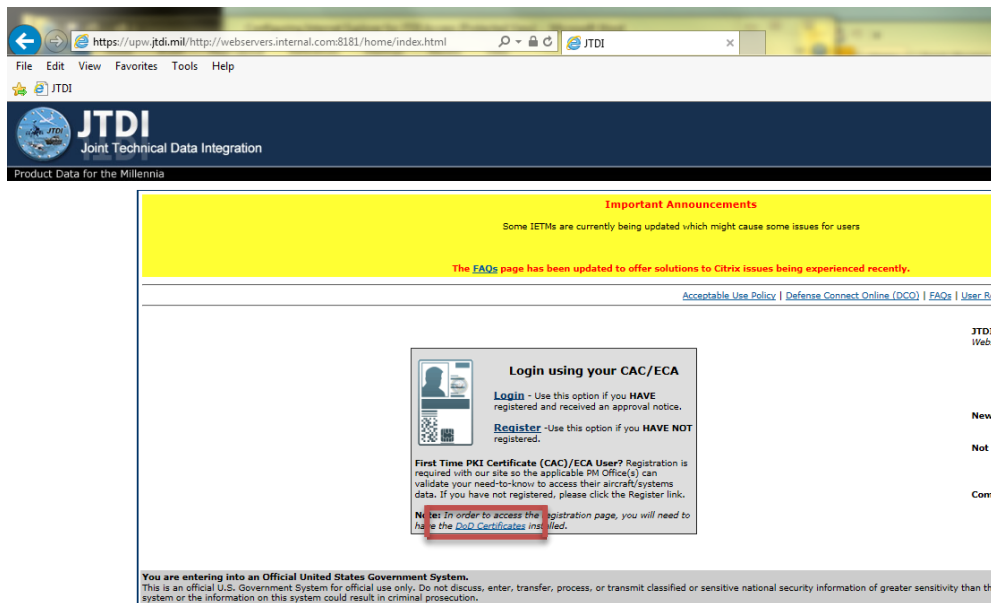
6. Select “Clear SSL state”, then “OK” on the following window to confirm.



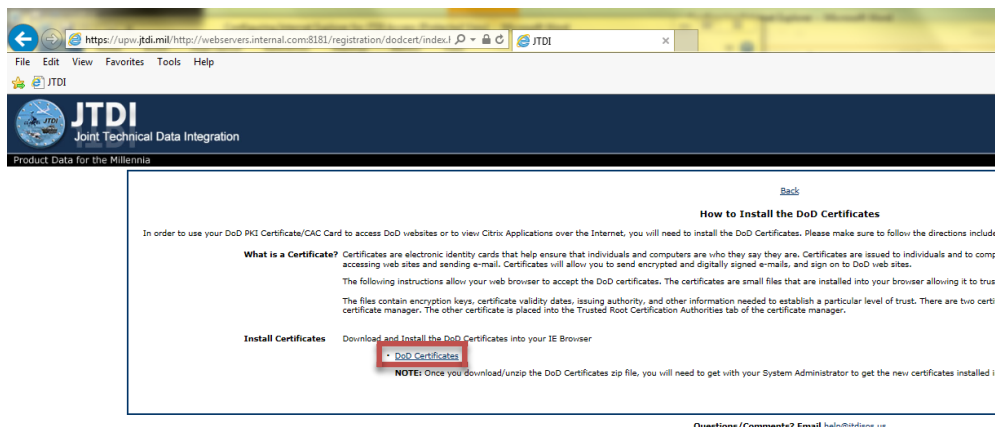
7. Select “Apply” and then “OK” – Close ALL Internet Explorer windows and then attempt to access <https://www.jtdi.mil>

***** If you have never before accessed the JTDI website please continue to step 11. If you have accessed in the past, please contact the helpdesk for further assistance. *****

8. Select “DoD Certificates”

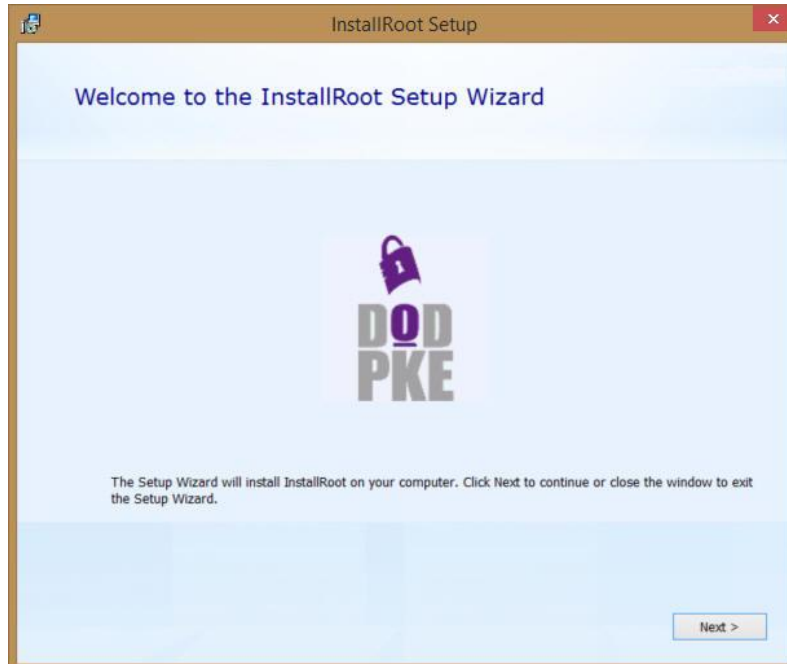


9. Select “DoD Certificates” once again after reading the “How to install DoD Certificates” instructions to download the InstallRoot 4.1.

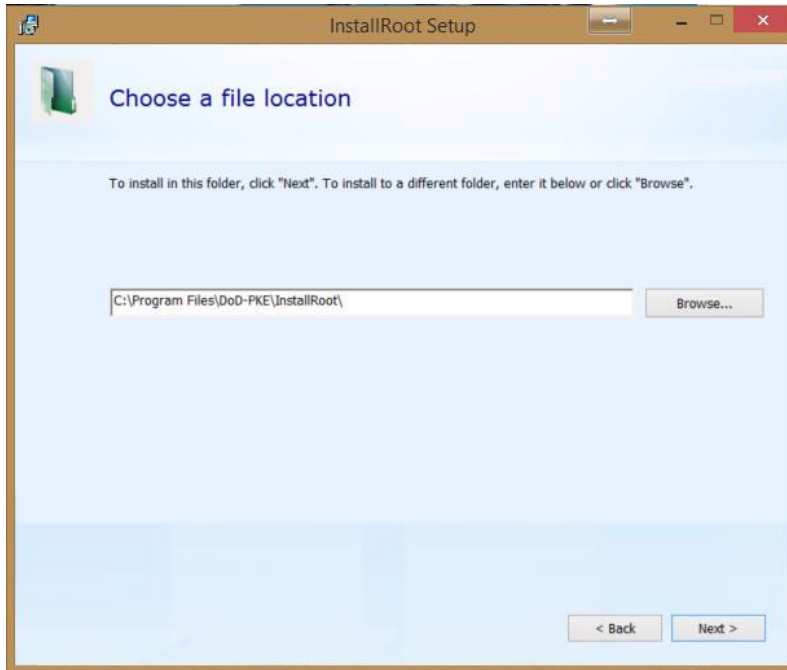


Direct link (URL: http://iasecontent.disa.mil/pki-pke/InstallRoot_NonAdmin_4.1.msi)

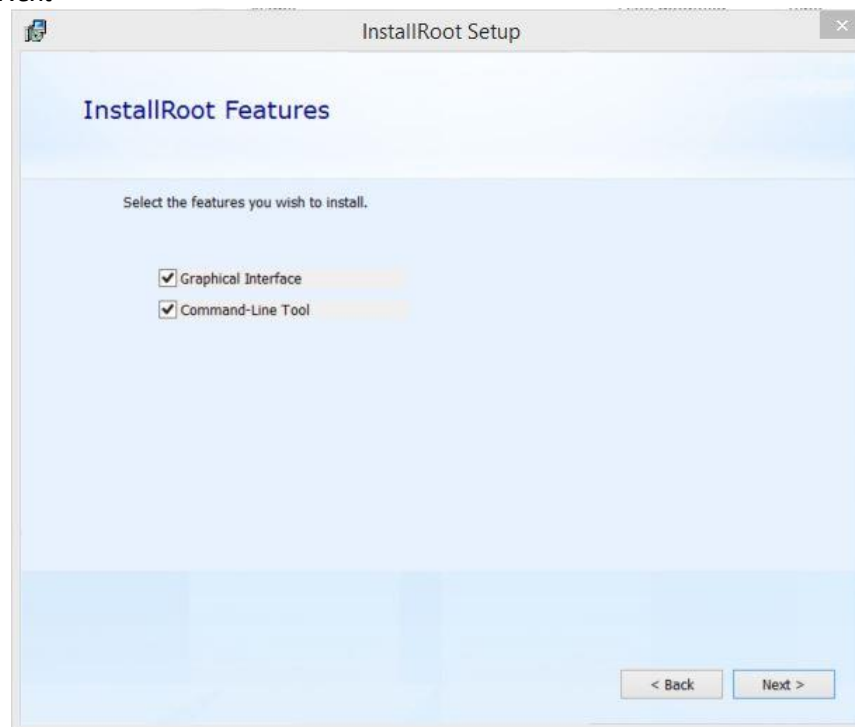
10. Select: *Next*



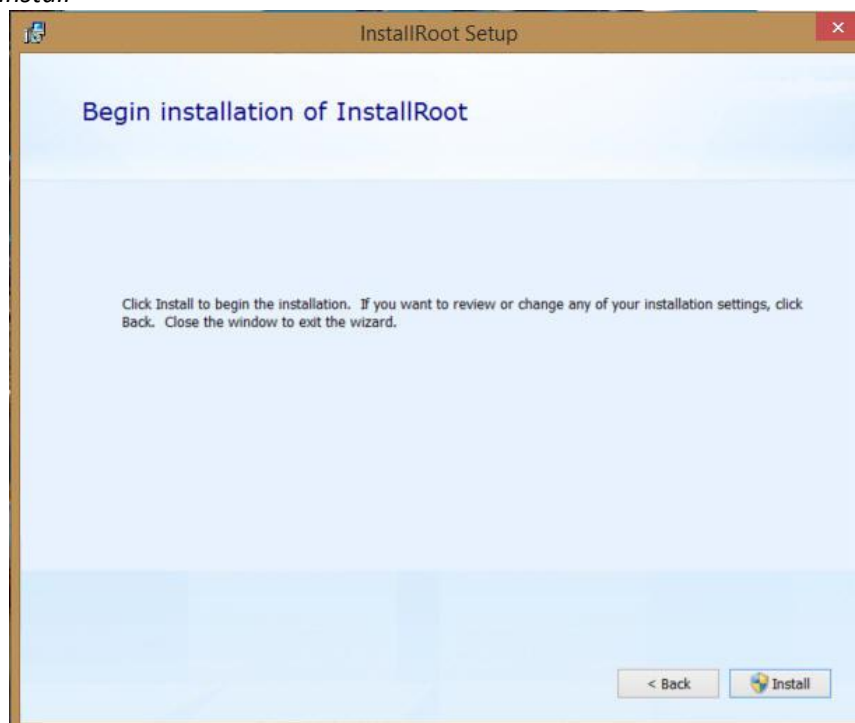
11. Select: *Next*



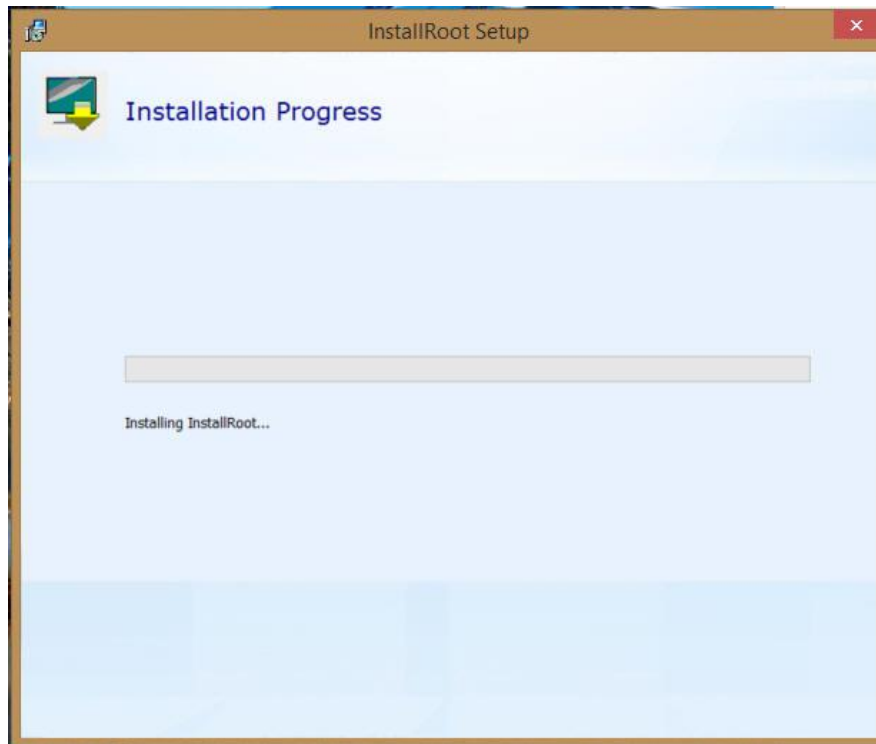
12. Select: *Next*



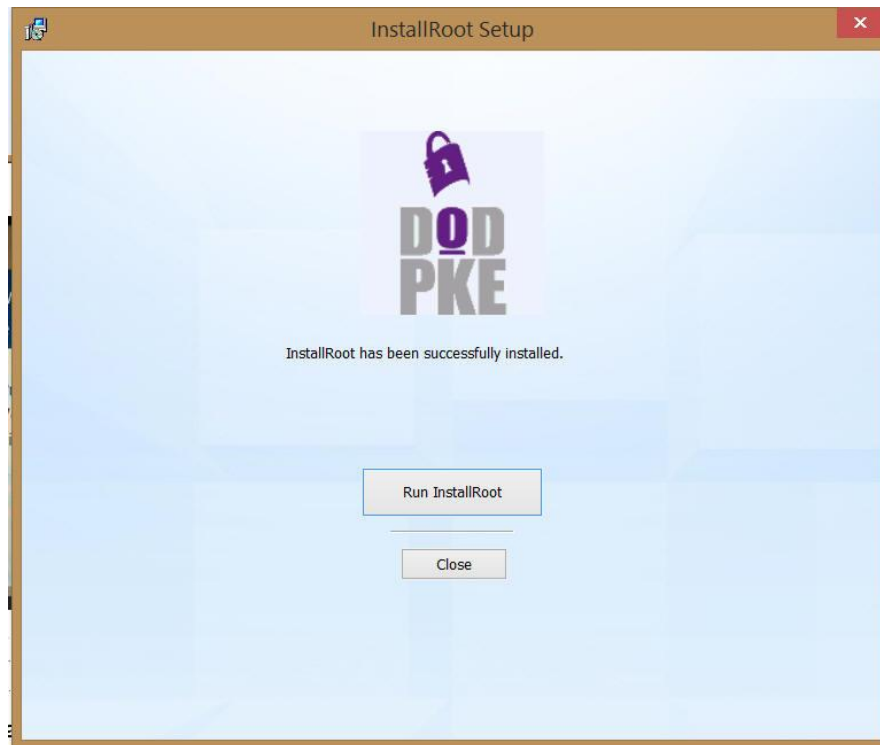
13. Select: *Install*



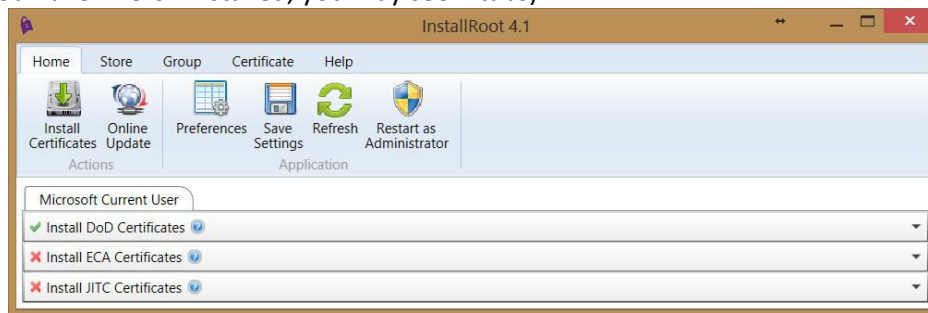
14. Wait for installation to start.



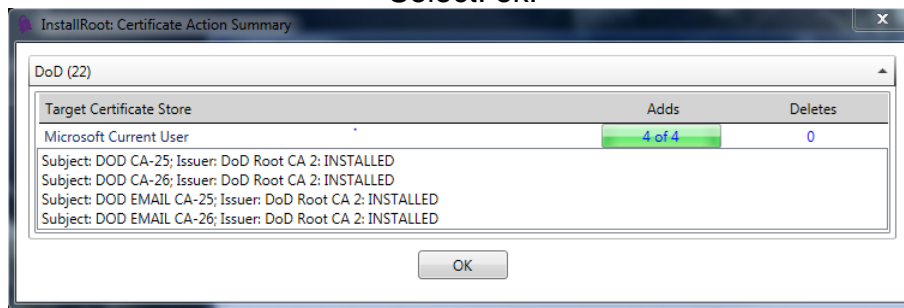
15. Select: *Run InstallRoot*



16. Click: *Install Certificates*
(If you have Firefox installed, you may see 2 tabs)



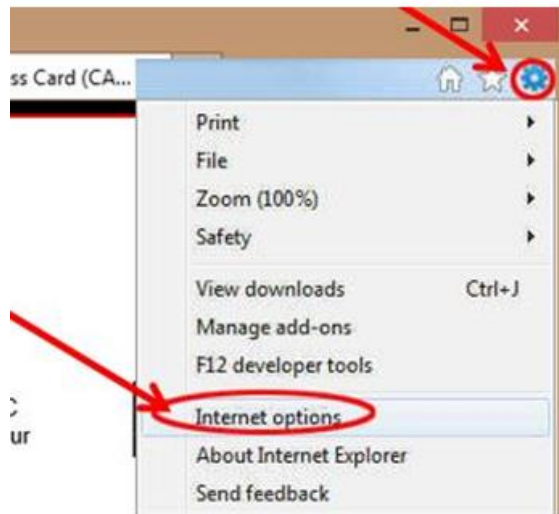
Select: ok.



17. Select Yes, (this screen may show 2 - 3 times)



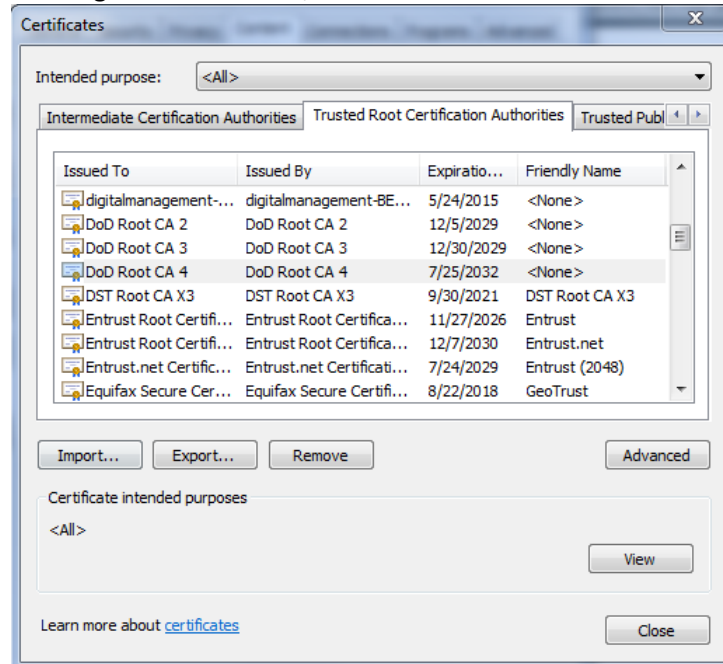
18. Open Internet Explorer, Select: *Tools, Internet Options*



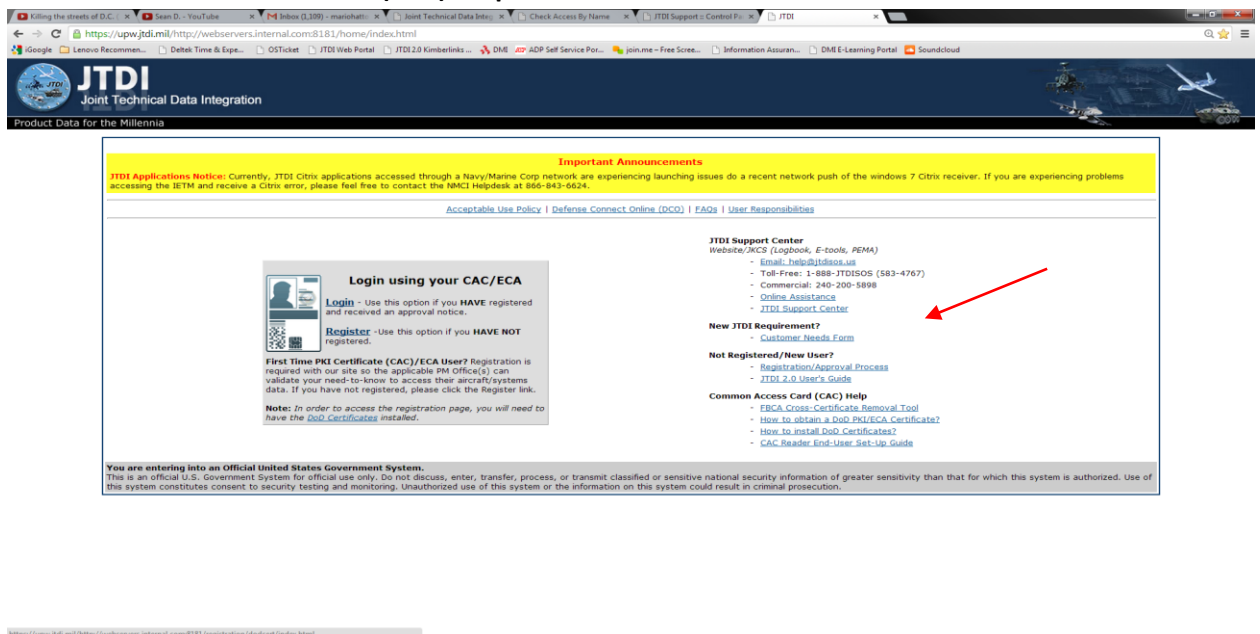
19. Select Content (tab), Certificates (button)



20. Open Trusted Root Certification Authorities (tab) to verify you have: *DoD Root CA 2* through *DoD Root CA 4*, and *DST Root CA X3*.



21. When complete go back to the login/register page, and on the right side of the page, in the column of text, select *FBCA Cross-certificate Removal Tool* located under the bolded header labeled **“Common Access Card (CAC) Help.”**



22. Select the DOD FBCA Cross certificate removal tool again located in the bottom left hand corner. Here you will need to download/unzip the FBCA Cross-Certificate Removal Tool zipped file to your desktop, then unzip and install the file.

Federal Bridge Certification Authority (FBCA) Cross-Certificate Removal Tool

To ensure that users do not experience denial of service when performing certificate-based authentication to DoD websites due to the system chaining to a root other than DoD Root CA 2, the Windows 7 STIG requires that the DoD Interoperability Root CA to DoD Root CA 2 cross certificate be installed in the Untrusted Certificate Store. This can be accomplished by running the FBCA Cross-Certificate Removal Tool which automatically installs the cross certificate into the Untrusted Certificate Store. Click the Intermediate Certification Authorities (tab) and look for the certificates shown below on the left graph.

Issued To	Issued By	Expiration
Common Policy	Common Policy	
DoD Interoperability Root CA 1	Sha-1 Federal Root CA	
DOD ROOT CA 2	DoD Interoperability Root CA 1	
Entrust	Common Policy	
Sha-1 Federal Root CA	Common Policy	
VeriSign Digital ID Certificate		Date is Expired

If the certificates above are found on your computer, you will need to download/unzip the FBCA Cross-Certificate Removal Tool zip file below and install:

- FBCA Cross-Certificate Removal Tool (May need to run as Administrator)
- Here is where the above file can be downloaded directly from DISA

Questions/Comments? Email help@jtdi.us

23. A DOS command prompt will appear prompting you to press enter.

```
C:\Users\mhatton\AppData\Local\Temp\Temp1_unclass-fbca_crosscert_remover_v108.zip\FBCA_cr...  
experiencing the issues.  
DEPENDENCIES:  
* Microsoft Windows 2000 SP3 or later Operating System  
* .NET Framework 2.0 or above  
USAGE:  
/HELP          This help screen.  
/SILENT        Silent mode - doesn't require user to hit <ENTER>.  
/LIST          Only List Certificates.  
/DISALLOW      Disallow the certificate before deleting it.  
/NODODROOT     Don't add the DoD Root CA 2 certificate to trust stores.  
/NOCPDISALLOW  Don't disallow the Common Policy Root certificates.  
/KEEPCP        Don't delete the Common Policy Roots.  
/ECA           Remove and untrust the ECA cross-certificate.  
/NODELETE      Do not delete any certificates.  
/FORCE         Add certificates regardless if they already exist.  
NOTE: Administrative privileges are required to remove certificates from  
the LocalMachine store.  
Specify a "/S" on the command-line will prevent this prompt.  
Press <ENTER> to continue...
```

24. When the install is complete you will see "finished" following by an admin warning. Press enter to finish. Once completed close and reopen you browser and attempt to log into JTDI.

